McAfee® Network Security Platform

[formerly McAfee® IntruShield®]

Release Version 6.0 Revision 1

(Document was revised on 12/13/10)

Software versions in this release

This document applies only to the following software versions.

Network Security Manager Image	*Signature set*	*Network Security Sensor M-8000, M-6050, M-4050, M-3050, M-1450, M-1250 Image*	*Network Security Sensor M-2750 Image*
6.0.7.9	6.4.13.23	6.0.7.7	6.0.7.20

You can use this version of the 6.0 Manager software to configure and manage the I-series Sensors, M-series Sensors, N-450 Sensors, and the NTBA Appliances.

Contents

1 What's new in this release 3

2 Issues resolved in this release 9
2.1 Resolved M-series Sensor software issues 9
2.2 Resolved Manager software issues 10

3 Known outstanding issues 11
3.1 Known M-series Sensor software issues 11
3.2 Known Manager software issues 12

4 Installation and upgrade notes 13

5 Technical assistance and problem reporting 14

6 More Information 15
6.1 About 6.0 Documentation 15

1 What's new in this release

This section details the features and/or enhancements delivered with this release of Network Security Platform 6.0.

All the features listed below are described in detail in Addendum II to 6.0 Documentation. Existing 6.0 guides are also updated to include the enhancements supported in this release. The sections below indicate the guide that contains updates for each feature/enhancement.

Heterogeneous Environment Support

With this release of 6.0, Network Security Manager provides support for a heterogeneous environment wherein Sensors configured with either 5.1 or 6.0 Sensor software can be configured to the 6.0 Manager. The signature set included in this release supports attack definitions for both 5.1 and 6.0, and hence provides a heterogeneous environment.

A 6.0.7.x Central Manager can support both 5.1.11.x and 6.0.7.x Managers. If your Central Manager setup has Managers using versions 6.0.3.x or 6.0.5.x, then you **must** upgrade all the Managers to 6.0.7.x to configure these to a 6.0.7.x Central Manager.

With a heterogeneous signature set, the Manager selects only the compatible attacks, signatures, and protocols based on the Sensor software. For example, for a 5.1.x Sensor, the Manager selects only the attacks, signatures, and protocols compatible for 5.1 from the heterogeneous signature set.

If you are upgrading from 5.1 to this release of 6.0, you need to manually import the heterogeneous signature set and push it to the Sensors.

With this release, the Manager can manage 5.1 and 6.0 I-series, M-series, N-450 Sensors, and NTBA Appliances.

A 6.0.7.5 Manager does not support NAC on both 6.0 and 5.1 I-series Sensors.

If you are upgrading from an earlier version of 6.0 and were using Snort signatures, and plan to add 5.1 Sensors to the same Manager, then after upgrading to this release of Manager software, perform the following steps:

1. In the Custom Attack Editor, go to File > Snort Advanced > View Snort Variables.
2. Click Re-Submit Rules using Current Variables.

A heterogeneous environment is useful in large deployments where the Sensor software upgrade to a major version can be handled in phases with minimum impact to the production network. McAfee recommends that you use the latest version of the Manager and Sensor software to avail all features supported in Network Security Platform version 6.0 onwards.

For more details, see 6.0 Upgrade Guide.

Update Server Authentication Enhancements

In earlier releases of 6.0, a separate authentication was required to access McAfee Update Server for downloading latest signature sets. With this release, upon a successful login to the Manager, you are automatically logged into the McAfee Update Server as well. Therefore, the Manager > Update Server > Credential page has been removed.

Licensing Changes

In this release of 6.0, the following licensing changes are available:

- You do not require a license file for using Manager/Central Manager version 6.0.7.x or above. Therefore, the Licenses tab under the Manager node has been removed.
- No license file is required for enabling IPS on I-series and M-series Sensors; no license is required for enabling NAC on N-450 Sensors. In other words, when you add a Sensor to the Manager, upon discovery, the native functionality supported on the Sensor model is automatically enabled.

- Like in earlier releases, you require an add-on license to enable NAC on M-series Sensors. Earlier, you could import the add-on license under Manager > Licenses tab. In this release, you can import/assign the license using the Device List > Add-On Licenses page.
- With this release, the Manager will not raise any fault on Sensor license expiry.

Refer to the Release Notes of the Manager version that you are installing or upgrading to for the latest information on licensing changes.

For details on configuring add-on licenses, see Device Configuration Guide.

Support for Active Fail-Open Bypass Kits

With this release of 6.0, Network Security Platform supports the following Active Fail-Open Bypass Switches:

- 10/100/1000 Copper
- 10/100/1000 Copper with SNMP Monitoring
- 1 Gigabit Optical – single and multi mode
- 10 Gigabit Optical – single and multi mode

When an Active Fail-Open Bypass Kit is configured and the Sensor is operating, the switch is “On” and routes all traffic directly through the Sensor. When the Sensor fails, the switch automatically shifts to a bypass state: in-line traffic continues to flow through the network link, but is no longer routed through the Sensor. Once the Sensor resumes normal operation, the switch returns to the “On” state, again enabling in-line monitoring.

During normal Sensor in-line fail-open operation, the Active Fail-Open Kit sends a heartbeat signal (1 every second) to the monitoring port pair. If the Active Fail-Open Kit does not receive 3 heart beat signals within its programmed interval, the Active Fail-Open Kit removes the Sensor’s monitoring port pair from the data path, and moves the Sensor into the bypass mode, providing continuous data flow.

When the Bypass Switch loses power, traffic continues to flow through the network link, but is no longer routed through the Bypass Switch. This allows network devices to be removed and replaced without network downtime. Once power is restored to the Bypass Switch, network traffic is seamlessly diverted to the monitoring device, allowing it to resume its critical functions.

Note the following:

- The Active Fail-Open Bypass kits can be configured for the following Sensor models: M-2750, M-3050, M-4050, M-6050, and M-8000.
- 10 Gigabit Active Fail-Open Bypass kits are supported only in 6.0.7.x version. Network Security Platform is yet to support 10 Gigabit Active Fail-Open Kits in the 5.1 version.
- With auto-negotiation mode on all speeds enabled, that is, if the first network switch is using a 10/100 Ethernet port and speed is auto and the second network switch is using a 10/100/1000 Ethernet port and speed is at auto, the maximum negotiable speed is 100Mbps. Therefore, configure the Sensor port pair to 100 Mbps auto-full and the Bypass Switch to remain at its default setting.
- Half duplex configuration is not supported on the Active Fail-Open Bypass Switch.

The Active Fail-Open Bypass Kit with SNMP monitoring provides the additional feature of raising SNMP faults to track events such as bypass state changes, threshold utilization, port link status changes, and power supply state changes.

For more details, see:

- 10/100/1000 Copper Active Fail-Open Bypass Kit Quick Start Guide
- 10/100/1000 Copper Active Fail-Open Bypass Kit with SNMP Quick Start Guide
- 1 Gigabit Optical Active Fail-Open Bypass Kit Quick Start Guide
- 10 Gigabit Optical Active Fail-Open Bypass Kit Quick Start Guide

Support for Concurrent Sensor Updates

In the earlier 6.0 releases, when multiple Sensors were configured to the Manager, Sensor software and signature updates were applied sequentially on each Sensor. In this release, the Manager provides an option for parallel processing of Sensor software and signature set updates.

Note: This option is available in the Device List > Device List > Software Upgrade page at the parent domain. The Sensor updates at the child admin domain must be performed using the same method as in earlier releases.

The Manager supports automatic refresh of the progress during the process. In the case of software upgrades, the Manager also provides the option to configure an automatic reboot of the Sensor once the new software is installed.

For details, see Device Configuration Guide.

Capturing Data Packets on the Sensor Port

Network Security Platform supports configuring a port of your Sensor to capture data packets on ingress traffic in your network, which can then be sent to an external device. Once captured, these data packets can be used to perform forensics analysis that help in identifying network security threats. Analysis of the captured data packets can help you monitor whether the data communication and network usage of your production environment comply with the outlined policies of your organization. The captured data packets can also be used for troubleshooting Sensor issues. Note that packet capturing is limited to the configured SPAN port alone.

Instead of configuring SPAN and TAP from third-party devices, packet capture in Network Security Platform can also be used to forward selected traffic [like HTTP, SMTP] to McAfee Data Loss Prevention and McAfee Network Threat Response.

Note the following:

- Network Security Platform supports packet capturing on M-series Sensor models only.
- Capturing of jumbo frame packets is also not supported.
- In case of a failover setup, each Sensor captures data packets separately.
- When a port is designated for capturing packets, it should not be used for IPS inspection.

Using the Manager, you can configure filter rules to capture packets based on protocols, VLAN ID, fragmented traffic etc. Rules can be set to capture packets on a single monitoring port or all ports.

Packet capture does not occur when:

- The Sensor is in layer 2 mode
- Scanning Exceptions is enabled on the Sensor
- Tunneling is enabled and the packet filter rule is set to any protocol (other than ALL), then tunneled packets that match the rule will not be captured

When the application protocol [like FTP, HTTP, DNS] filter rules are configured and the Sensor receives fragmented traffic matching these filter rules, the Sensor captures only the first fragmented packet of the flow and not the subsequent ones. This is because the port information is present in the first fragment alone.

McAfee recommends that you ensure that the capture traffic volume is less than the capacity of the configured capture port of the Sensor. Otherwise, this can affect the Sensor performance.

For details, see Device Configuration Guide.

Vulnerability Manager Integration Enhancements

With this release, the Manager supports integration with Vulnerability Manager version 7.0 as well.

In the earlier versions of Manager, Vulnerability Manager integration with the Manager was possible only at the root admin domain level. With this release, Vulnerability Manager integration can be enabled at root as well as child admin domains.

Earlier, on-demand scans from the Threat Analyzer Host Forensics page was not child admin domain-specific. With this release, you can also select the child admin domains for which you want to execute a scan.

For details, see Integration Guide.

Integration with McAfee Global Threat Intelligence

McAfee Global Threat Intelligence [GTI] is a global threat correlation engine and intelligence base of global messaging and communication behavior. McAfee GTI has two components namely, Artemis and TrustedSource. McAfee Artemis provides file reputation whereas McAfee TrustedSource can provide:

- Web reputation
- Web categorization
- Message reputation
- Network connection reputation

McAfee Network Security Manager integrates with McAfee GTI to support the following:

- **TrustedSource integration for reputation scores**: Obtain the reputation and geo-location for each host involved in an attack (both source and destination). The Manager maps the country codes received from TrustedSource to country names, and displays in the Threat Analyzer Alerts page.

  Important: In most cases, reputation shown on the Threat Analyzer Alerts page will be different from the information shown by the right-click query option on a specific alert. This is because the TrustedSource web-site displays web reputation and mail reputation. The reputation displayed on the Manager however, is the network connection reputation, which is based on a combination of the IP address and protocol/port. Note that the Threat Analyzer displays web reputation for a destination IP if the destination port is 80. Likewise, mail reputation is shown for a source IP if the destination port is 25.

- **GTI Participation**: When participation is enabled, you can choose to configure the Manager to periodically send the following data to McAfee Labs: alert data detail, alert data summary, general setup, and feature usage. McAfee Labs then uses this data for global threat analysis to provide customers with aggregated data and enhanced threat information.

When you log onto the Manager for the first time, the GTI Participation page is displayed as part of the Manager Installation Wizard. You can opt to participate in GTI by setting your preferences in this screen. By default, all the options are **enabled**. If you decide to skip making any selection, the Manager will send a reminder after 30 days for enabling GTI participation.

Important: You must select either **Alert Data Details** or **Alert Data Summary** as “Yes” to enable TrustedSource integration.

Based on your selection(s), the Manager periodically sends the following data to McAfee Labs:

- **Alert data detail**: this provides a complete integration with TrustedSource. When this option is enabled, the Manager sends detailed data on alerts, alert summary and general information like Manager and signature set version. The Manager supports configuring a CIDR exclusion list to prevent alert data details from being shared with TrustedSource for specific hosts.

  You must enable this option to view data in the following columns of the Threat Analyzer Alerts page:
  - Dest Country
  - Dest Reputation
  - Src Country
  - Src Reputation

- **Alert data summary**: Selecting this option also enables integration with TrustedSource. When enabled, the Manager sends alert summary and general information like Manager and signature set version to McAfee Labs.

  You must enable this option to activate the Threat Analyzer right-click menu option on each alert to query McAfee's http://www.trustedsource.org web-site for details of the source or destination host based on the IP address.

- **General setup**: Selecting this option will send general information about your setup to McAfee Labs.

- **Feature usage**: When you select this option, feature usage information from your setup will be sent to McAfee Labs.

If you chose to skip enabling GTI participation during your first login, then you can also configure these options from the Manager Resource Tree under Integration > Global Threat Intelligence.

For details, see Integration Guide.

Setting the Scanning Exceptions

With this release of 6.0, Network Security Platform supports configuring scanning exceptions from the Manager to bypass IPS inspection of traffic from a configured VLAN, TCP, or UDP port. The scanning exceptions configurations can be enabled/disabled at the Sensor level. If either the source or destination matches the specified value, scanning will be bypassed.

Earlier this feature was supported using the following Sensor CLI commands:

- layer2 forward tcp <enable | disable><0-65535>[<0-65535>]
- layer2 forward udp <enable | disable><0-65535>[<0-65535>]
- layer2 forward vlan <enable|disable> <0-4095> [<0-4095>]
- layer2 forward vlan <enable|disable> <0-4095>[<0-4095>] <interface <all|interfaceA-interfaceB>>
- layer2 forward clear

Note the following:

- Scanning exceptions is supported only in the following M-Series sensor models: M-8000, M-6050, M-4050, M-3050, and M-2750.
- Scanning exceptions rules can be configured on ports running in inline mode. Once set, these rules take precedence over ACLs.
- Fail-over ports and M-8000 interconnect ports cannot be configured for scanning exceptions.
- In a fail-over pair, scanning exception rules are applied to both the Sensors. On creation of a fail-over pair, the Primary Sensor rules are copied to the Secondary Sensor.
  With this release, layer2 forwarding is supported from the Manager. A minimum Sensor software version of 6.0.7.x or above is required to support this feature in the Manager. On upgrade of the Sensor software version to 6.0.7.x, the Manager copies and stores the existing rules from the Sensor. It occurs only once for handling the old rule configured in the Sensor through the CLI. After upgrade, you cannot configure scanning exceptions on the Sensor through the CLI.

For details, see IPS Configuration Guide.

Policy Editor UI Enhancements

The UI for the IPS Settings > Policies > IPS Policies page has been enhanced to simplify access and manipulation of attack definitions with options such as sorting, group by, and filter management. Note the following changes:

- The Add button in the IPS Policies page has been renamed to New. When you click New, the Policy Details window is displayed. The Policy Details window has two tabs namely, Properties and Attack Definitions.
- From the IPS Policies page, you can select an attack and double-click or use the right-click menu to edit, bulk edit, or enable/disable an attack.
- You can add a single attack set or different attack sets for Inbound/Outbound attacks. On clicking “Calculate Attack Definitions”, the attacks are loaded into the Attack Definitions tab of the Policy Details page. Attacks from both Inbound/Outbound and across all the categories are displayed.
- A new option called Filter Management is available to filter and view attacks for a selected policy.
- A Quick Filter option is also provided to search attacks. When you enter the search criteria and click “Save”, the Quick Filter is converted to an Advanced Filter. The Advanced Filter option enables the user to search attacks based on several complex criteria.
- A Group By option is supported to group attacks based on specific parameters. Drilldown option is also provided.
- Data in Columns like Responses and Notifications are displayed as icons.
- The Applications column provides a count of applications relevant for a particular attack.

For details, see IPS Configuration Guide.

Support for Import of NAC Exclusion List from a File

With this release, you can add items like IP addresses, IPv4 networks, MAC addresses, OUIs, and Network Objects to the NAC Exclusion List. If you have a long list of heterogeneous items to add to the NAC Exclusions List, consider using a CSV file. For example, consider having to add some 100 IPv6 addresses, 100 MACs, 10 OUIs, and 200 IPv4 addresses one by one to the NAC Exclusion List. Instead, you can store them all as comma-separated values in a CSV file and import them into the Manager. The successfully imported items are appended to the current NAC Exclusion List.

You can import the CSV file using the NAC Exclusions page in the NAC Configuration Wizard or the IPS Quarantine Wizard.

For details, see NAC Configuration Guide.

Automatic Custom Role Synchronization between an MDR pair

From this 5.1 release, custom role synchronization is performed automatically between an MDR pair. Custom roles created on the Primary Manager are automatically copied onto the Secondary Manager.

If you have a Central Manager setup, then custom role synchronization between the Central Manager and the Manager also happens automatically.

For details, see Administrative Domain Configuration Guide.

Alert Synchronization between an MDR pair

When the Sensor detects a transmission that is violating the security policy of the network, it generates a data on such transmission. This data or 'alert' is sent to the Manager, which in turn is acknowledged for storage or marked for deletion.

The actions that are triggered on these alerts from the active Manager are synchronized with the standby Manager in real time. This ensures minimal loss of data if the active Manager goes down.

For details, see Manager Server Configuration Guide.

Renaming of Threat Analyzer UI Components

Earlier you could launch the Threat Analyzer from the Homepage by making your selection from a drop-down list and clicking the Launch button. With this release, the Home page UI has been enhanced to include two new menu items:

- Real-time Threats – click to open Real-time Threat Analyzer
- Historical Threats – click to open Historical Threat Analyzer

In Threat Analyzer, the following views have been renamed:

Previous terminology	*New terminology*
Summary	Dashboards
General	NSP Health

For details, see System Status Monitoring Guide.

Viewing URL information for exploit alerts

When you receive an exploit alert in the Threat Analyzer, you can right-click to view the alert details. With this release, the details of an alert also include the target URL for server targeted attacks. The URL is displayed only for http alerts. For any non-http request, a blank area (----) will appear in the text area.

Note: Display of URL is disabled by default. Refer KB69333 for enabling this option.

You can generate the Next Generation Default – Attack URL Info report to view a list of the URL information.

The Threat Analyzer does not support display of URLs for attacks containing jumbo frame packets.

For details, see System Status Monitoring Guide.

Manual Quarantine of a Host from the Threat Analyzer

Using the Threat Analyzer, you can now manually quarantine a host even before it is detected on the network. Note the following:

- You can manually quarantine a host only on ports where IPS Quarantine is enabled.
- This is not applicable to NAC-only Sensors.

You can click the 'Quarantine' button on the Alerts or Hosts page to use this option.

For details, see System Status Monitoring Guide.

Reports

The following new Next Generation Reports are supported:

- Default - Global Threat Intelligence
- Default - Source Reputation Summary
- Default - Top 10 Attack Destinations
- Default - Top 10 Attack Sources
- Default - Top 10 Source Country

The following new Configuration Report is supported:

- Scanning Exceptions Report

For details, see Reports Guide.

Manager Infrastructure Enhancements

With this release, the Manager provides the following infrastructure enhancements:

- Both 32 bit and 64 bit Internet Explorer [IE] 8.0 are supported for viewing the Manager pages along with IE 7.0. Note that IE 6.0 is no longer supported.
- Server-side JRE is upgraded to version 1.6.0_20
- Apache httpd is upgraded to version 2.2.16
- In earlier release of 6.0, all Manager database tables used InnoDB storage engine except alert data and packet log tables. With this release, alert data and packet log tables are also converted to InnoDB.

2 Issues resolved in this release

The following table contains issues resolved in this release of Network Security Platform 6.0.

2.1 Resolved M-series Sensor software issues

The issues listed below are addressed in Sensor model M-2750 alone.

High severity Sensor software issues

ID #	*Issue*
621981	The Sensor ports configuration changes during Sensor operation and this can cause Sensor to stop

High severity Sensor software issues

ID #	*Issue*
	processing traffic.
626386	On rare occasions, when Artemis is enabled, the Sensor could reboot due to a data path error.

Medium severity Sensor software issues

ID #	*Issue*
630071	Enabling latency monitoring is not persisted across reboots.
624154	On rare occasions, after signature download, the Sensor could report false positives.
622689	With high volume of correlated alerts, packet logs may be missed for some of the Exploit alerts.

2.2 Resolved Manager software issues

Medium severity Manager software issues

ID #	*Issue*
630051	Unable to view new alerts in the Threat Analyzer after running the Manager a while. In an MDR setup, the new alerts are seen only in one of the Managers.
630054	Upgrade to JRE 1.6.0 update 22 for all Manager components.
627473/ 626768	After an upgrade from 5.1.17.x to 6.0.7.5, the Manager is unable to communicate with the Update server via a proxy server. That is, upon upgrade, the proxy settings are automatically disabled.
626663	Unable to add an NTBA Appliance to a Manager upgraded from 5.1 to 6.0.
624583	Unable to edit and save changes to LDAP users.
624472	After an upgrade to the latest Manager, signature set update failed.
621840	Unable to delete the NTBA Appliance from the Manager when there proxy server setting is enabled.
616800	[NTBA] In an NTBA aggregator setup, the Applications Traffic monitor does not display any data.
616251	[NTBA] Getting number format exception and no data is shown on issuing "Host Profile" query for the external host from the generated alert.
615904	[NTBA] Top Source Host monitor displays only 20 entries instead of the configured value.
615824	[NTBA] Top N value for a custom monitor is limited to 100.
615530	[NTBA] The Application Traffic summary query under HTF monitor is not sent to the correct NTBA Appliance when configured in aggregator.
615254	[NTBA] The Interface speed for M-8000 Sensor is sent as 0 to NTBA.
592334	A default Next Generation report defined at the root admin domain level can be viewed from the child admin domain level but the report result is not specific to the child domain.
592329	In the Threat Analyzer, users restricted to a sub-domain are able to view the incident generator reports for Sensors belonging to other domains.

Medium severity Manager software issues

ID #	*Issue*
590261	The Threat Analyzer freezes when a user tries to group alerts by source or destination IP.
590257	In the Threat Analyzer, when IPs are added to manually quarantine a host, the IPs are not listed in the Hosts page.
589633	When the automatic download of signature sets to the Sensor is disabled, the Manager continues to push signature sets to the Sensors.
586611	The Performance Monitoring - Sensor Configuration Report generation for a failover pair results in an internal application error.
584015	The user-defined report for port data rate display values in bps unit instead of Kbps/Mbps/Gbps units.
568567	[NTBA] A particular zone level policy violation rule is being pushed to all zones causing alerts to be raised for all zones even when those zones do not have that rule configured.
562441	[NTBA] The fault for NTBA DB Tuning is shown under warning. The fault should be shown under informational.
559883	The Group by interface option in the Threat Analyzer does not show the interfaces of both the Sensors connected to the Manager.
547337	The Executive summary report generation fails intermittently.

3 Known outstanding issues

The following tables contain the known, outstanding issues for this release of Network Security Platform 6.1.

For issues discovered later and/or not mentioned in the Release Notes, refer to https://kc.mcafee.com/corporate/index?page=content&id=KB65523

3.1 Known M-series Sensor software issues

High severity Sensor issues

ID #	*Issue*	*Workaround*
537281	[M-8000] Attack detection is not happening for IP in IP tunnel packets.	None
526382	Rate limiting does not work on M-8000 S ports.	None

Medium severity Sensor issues

ID #	*Issue*	*Workaround*
621116	Changes to packet log encryption settings from the Manager do not take effect until a Sensor reboot or reconnect of the channels.	Manually disconnect/reconnect the channels using CLI commands when these settings are changed.
537012	[Snort] The Sensor does not raise an alert when a space is part of the	Separate into multiple content

Medium severity Sensor issues

ID #	*Issue*	*Workaround*
	content matching rule.	keywords in a single rule.
530949	The diffserv functionality does not work for ICMPv6.	None
519881	[Snort] When the number of fields to match in non payload options is more than 5, the Sensor does not raise an alert.	Create separate rules limiting non payload options to 5 in each rule.

3.2 Known Manager software issues

High severity Manager issues

ID #	*Issue*	*Workaround*
622246	When a fail-over pair is added to the Manager at the child domain level, and the port settings are changed on any one of the Sensors, the Manager throws an unexpected error.	1. From the Resource tree pane, click the "Return to Previous Page" link. 2. Select the fail-over Sensor_Name node. 3. Go to "Configure Update", and click "Update" to update configuration to the Sensors.
621735	During a Manager login using CAC, multiple pop-ups are received for selecting the CA certificate.	Re-doing the CA certificate selection multiple times addresses this issue.
536543	In rare cases due to race conditions, simultaneous import of multiple Sensor software images into the Manager could cause the images to get corrupted.	Call McAfee support to clean up the database, and re-import the Sensor software image.
519900	The Incident Generator does not generate incidents.	None

Medium severity Manager issues

ID	*Summary*	*Workaround*
622756	When both TrustedSource integration and display of URL information are enabled, the URL information is missing in the Show Details window, and the Historical Threat Analyzer.	None
622245	In a heterogeneous environment, a 6.0.7.5 Central Manager does not support Managers running software version 6.0.3.x or 6.0.5.x.	Upgrade all Managers in your setup to 6.0.7.5.
621840	Unable to delete an NTBA Appliance from the Manager when proxy is enabled.	Delete proxy settings from NTBA and then delete the Appliance from the Manager.
621785	Editing attacks at both the policy and GARE levels from the Central Manager Threat Analyzer throws an error.	Edit the policies from the Policy Editor page.
620604	[NTBA] The ‘quarantine until explicitly released’ option is not working for hosts quarantined by NTBA.	None

Medium severity Manager issues

ID	*Summary*	*Workaround*
611493	[NTBA] When the user adds the host to quarantine from Alerts page for a host, no 'Host already exists' message is shown for an existing host. Instead the Threat Analyzer extends the quarantine duration.	None
522320	[Custom attacks] In Show details for UDS/Snort alerts, the sub category is shown as "unassigned" and Detection mechanism as "0".	None
475945	[NAC] On changing the NAZ policy on the Threat Analyzer for a VPN Host, the new NAZ policy name is not dynamically updated on the Threat Analyzer, but gets correctly updated on the Sensor.	Restart the Threat Analyzer.
454399	[IPS] "Synchronization Required" (Manager List -> Policy Synchronization tab) status is not becoming true when Alert filters / Rule Sets are created in the Central Manager after upgrade. Reason column also remains blank.	None
432613	[NAC] The backup AD for a domain in the user identity store is not used for role derivation lookup if the primary AD for the same domain is down.	None
307619	[IPS] In Alert Manager, description for Host Intrusion Prevention alerts is blank.	None.
231052	Archive files larger than 4GB become corrupted due to .ZIP file format limitations.	Any time you create an archive, validate the archive on a separate machine before deleting alerts and packet logs that have been archived. An archive file larger than 4GB is very likely corrupted.

Low severity Manager issues

ID #	*Issue*	*Workaround*
508671	[NTBA] The Edit attack response option is not available for NTBA alerts.	None
431480	The Threat Analyzer displays the session time as "Not Available" for quarantined hosts after a Sensor reboot.	None

4 Installation and upgrade notes

Review the following before you install the Manager software:

You can use any one of the following OS for installing the Manager:
- Windows Server 2003 Standard Edition, SP2 (32 or 64 bit), English OS
- Windows Server 2008 R2 Standard Edition, (64 bit), English OS
- Windows Server 2003 R2 (Standard Edition), Japanese OS (32 or 64 bit)
- Windows Server 2008 R2 (Standard Edition), Japanese OS (64 bit)

The Manager server should have a minimum of 2 GB memory. McAfee recommends using 4GB memory on the Manager server for optimal performance.

Only Windows XP (SP2) and Windows 7 clients are supported using Internet Explorer 7.0 or 8.0 to view the Manager.

The Manager client should have a minimum of 1 GB memory for accessing the Manager. McAfee recommends using 2GB memory on the Manager client for optimal performance.

For more details, see Installation Guide.

McAfee regularly releases updated versions of the signature set. Note that automatic signature set upgrade does not happen. You need to manually import the latest signature set and apply it to your Sensors.

The following table provides the Network Security Platform components versions supported for upgrading to this release of Sensor and Manager software:

Manager image	*Central Manager image*
6.0.1.5 or above	6.0.1.5 or above
5.1.11.25 or above	5.1.11.25 or above

M-8000 Sensor Image	*M-6050, M-4050, M-3050, M-2750 Sensor Image*	*M-1450, M-1250 Sensor Image*
6.0.1.5 or above	6.0.1.5 or above	6.0.1.5 or above
5.1.7.74, 5.1.11.38, 5.1.11.54 or above	5.1.7.74, 5.1.11.38 or above	5.1.7.73, 5.1.11.38 or above

For more details, see Upgrade Guide.

5 Technical assistance and problem reporting

Technical support may request certain information from you to assist you in troubleshooting. A description of this information is provided in Troubleshooting Guide.

On-line

Contact McAfee Technical Support at http://mysupport.mcafee.com

Registered customers can obtain up-to-date documentation, technical bulletins, and quick tips on McAfee' 24x7 comprehensive KnowledgeBase. In addition, customers can also resolve technical issues with the online case submit, software downloads, and signature updates.

Via Phone

Technical Support is available 7:00am to 5:00pm PST Monday-Friday. 24x7 Technical Support is available for customers with PrimeSupport Priority or Enterprise service contracts.

Phone: 1-800-338-8754 (US Toll Free) or +1.972.963.8000 (Outside US)

Note: McAfee requires that you provide your GRANT ID and the serial number of your system when opening a ticket with Technical Support. You will be provided with a username and password for the online case submission.

6 More Information

6.1 About 6.0 Documentation

To view the complete Network Security Platform 6.0 Documentation,

1. Go to http://mysupport.mcafee.com/Eservice/
2. Click 'Read Product Documentation'.
3. To view sensor related information, under 'Product' categories, select:
   - Network Security Sensor Hardware - select the Sensor model number
   - Network Security Sensor Software - select the version as 6.0
4. Similarly, to view Manager related information, under 'Product' categories, select:
   - Network Security Manager Software

Refer the table below if you are looking for more information on Network Security Platform 6.0:

Information regarding…	*Where can I find?*
Information on the immediate previous Network Security Platform releases: ▪ 6.0.1.5-6.0.1.5 [I-series, M-series] ▪ 5.1.11.10-5.1.7.74 / 5.1.7.73 [M-8000, M-6050, M-4050, M-3050, M-2750 / M-1450, M-1250] ▪ 5.1.11.10-5.1.5.90 [I-series]	Go to http://mysupport.mcafee.com/Eservice/ > Read Product Documentation > Network Security Sensor Software / Network Security Manager Software. Look for Release Notes marked with the released Sensor and Manager software versions in the title.
Sensor/Manager/Signature Set requirements	Manager Installation Guide
Sensor requirements	Refer the corresponding Sensor Product Guide for the sensor model that you have purchased.
Compatibility with 3rd-Party tools	Installation Guide
Database requirements	Installation Guide
Manager system and client requirements	Installation Guide
Additional server requirements	Installation Guide
License requirements	Installation Guide
Upgrade instructions	Upgrade Guide
CLI commands for Sensors	CLI Guide
Supported protocols list	Go to http://mysupport.mcafee.com/Eservice/ > Search the KnowledgeBase > KB61036
Providing a diagnostics trace for a device	Troubleshooting Guide